



Document Downloaded: Tuesday November 10, 2015

Joint AAU and COGR Letter to NIST on Controlled Unclassified Information

Author: AAU and COGR

Published Date: 01/22/2015

January 16, 2015

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930

Subject: NIST Special Publication 800-171

Dear Sir,

On behalf of the Council on Governmental Relations (COGR) and the Association of American Universities (AAU), we write to comment on the NIST Special Publication 800-171. COGR is an association of 189 U.S. research universities and their affiliated academic medical centers and research institutes that concerns itself with the impact of federal regulations, policies, and practices on the performance of research and other sponsored activities conducted at its member institutions. AAU is an association of 60 U.S. and two Canadian preeminent research universities organized to develop and implement effective national and institutional policies supporting research and scholarship, graduate and undergraduate education, and public service in research universities.

We appreciate the recognition in NIST Special Publication 800-171 that federal agency information security requirements are inappropriate for nonfederal organizations, and that equivalent security solutions can be implemented to satisfy security requirements. We also appreciate acknowledgement of the need to reduce complexity for federal contractors and to promote standardization to benefit nonfederal organizations that are confronted with differing contract requirements from federal agencies. This has been a problem for our member institutions, particularly the inconsistent implementation of Federal Information Security Management Act (FISMA) requirements by federal agencies.

However, both of our Associations have long been concerned about the proliferation of federal requirements pertaining to sensitive, unclassified information (now *Controlled Unclassified Information* (CUI) pursuant to Executive Order 13556), particularly with regard to basic and applied research conducted at our member institutions. Such requirements are inconsistent with basic federal policy set forth in National Security Decision Directive 189 (NSDD-189). That policy, reaffirmed by every subsequent Administration since it was originally issued in 1985, states "...to the maximum extent possible, the products of fundamental research remain unrestricted. It is also the policy of this Administration that, where the national security requires control, the mechanism for control of information generated during federally-funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification...No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. Statutes." The policy is incorporated in the FAR at 48CFR27.404-4(a).

We are therefore particularly concerned that in the introduction to the draft Special Order 800-171 (page 1), the first example given of sensitive unclassified federal information in contractor information systems is the conduct of basic or applied scientific research. That implies a basic misunderstanding of federal policy.

We also question the premise that such information typically is “federal information,” a term which is not defined in the Special Order’s glossary. In our view, any such information that is not owned by the federal government or required to be delivered as a contract deliverable is not “federal information.” The glossary definition of “federal information system” also is unclear. Use of an information system by a university for a federally-funded research contract does not necessarily make that system a “federal” information system, or a system operated “on behalf of an executive agency.” Much information generated through federally-funded research or subject to a variety of federal regulatory requirements resides on or transits university information systems, but is not owned or controlled by the federal government. We suggest that NIST clarify the scope of “federal information” and “federal information systems” for these purposes.

Most of our member institutions focus on the performance of fundamental research and try to avoid or limit accessing or maintaining CUI. This is not always possible, especially given the proliferation of CUI requirements by federal agencies. While we understand that designation of CUI is not NIST’s responsibility, it would be useful for the guidance to reiterate the EO 13556 provision 3.b. that “If there is significant doubt that information should be designated as CUI, it shall not be so designated.” It also would be useful to include a specific waiver process from the CUI requirements, perhaps at the end of the last bullet on page vii (“.....or present justification to request for a waiver to be granted from such requirements for a specific scenario”).

The federal government’s plan for implementation of the CUI program envisions three parts: a CUI rule issued by NARA for uniform controls and marking; the NIST standards for security requirements; and a FAR rule to apply the requirements to contractors. Without the ability to review the two planned rules, it is difficult to fully assess the impact of these requirements. However, we anticipate additional burdens will be incurred by our member institutions. The standards will create additional work for universities that already use ISO standards as their security framework and not NIST. Additionally, there are concerns about the need to formalize campus information security risk management/assessment practices to meet the requirements in NIST 800-53 and 800-171. Some of the controls may be very challenging to implement for large decentralized universities. And finally, there is some confusion regarding whether the controls are required or need only be applied based on identified risks.

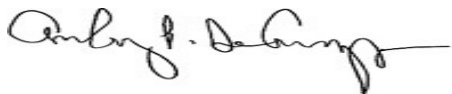
800-171 sets forth fourteen “families” of security requirements with over 100 listed controls derived from requirements for federal systems from NIST Special Publication 800-53. This number is rather staggering. A specific example of added burden is the derived security requirement in 3.5a. for use of multifactor authentication for local and network access to privileged and non-privileged accounts. Requiring multifactor authentication for network access to non-privileged accounts will be an organizational cost overhead where two-factor authentication is achieved usually by using tokens ('something you have'). For researchers who have non-privileged accounts the number of tokens and the infrastructure to maintain the cost of such hardware could be burdensome for the organization and add costs to the project.

All of our member institutions have established information security requirements and are very familiar with the need to protect information system infrastructure and processes. 800-171 appropriately recognizes that small business contractors may have difficulty in meeting the requirements. In fact, they may drive researchers (working with CUI) from small research labs to outside servers that are professionally managed. However, in all cases 800-171 implies that CUI should be handled outside a contractor's normal information system. This suggests the need to explicitly recognize the related costs as direct costs in project budgets. Otherwise the result will be another unfunded mandate which adds additional costs and burdens for our institutions.

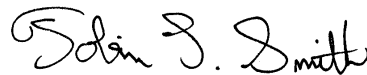
While 800-171 encourages proposals of alternative security solutions by nonfederal organizations, we are concerned that the 800-171 standards are likely to become prescriptive, and that the recognition of alternative equivalent methods is likely to be lost, particularly once the rule is issued in the FAR. The onus also needs to be on the federal agency to clearly state in the solicitation and contractual documents when CUI is involved and when the standard is invoked (as well as that costs of compliance with the CUI requirements may be included as direct costs). It would be very troublesome if it becomes a clause that is automatically prescribed in all government contracts. We believe NIST needs to clarify the scope of this guidance by clearly indicating that the 800-171 controls are intended to be illustrative and not necessarily prescriptive or applicable in all cases. We also urge that the NARA rule and FAR clause recognize these distinctions. We have reviewed the draft comments of the Association of University Export Control Officers and generally concur in those comments, particularly with regard to export-controlled information and fundamental research.

We appreciate the opportunity to comment, and would welcome the opportunity for further discussion.

Sincerely,



Anthony P. DeCrappeo
President
Council on Governmental Relations



Toby Smith
Vice President for Policy
Association of American Universities